Claims

WE CLAIM:

1. A method comprising:

receiving a manifest defining a plurality of code assemblies that are members of at least one application;

evaluating application evidence for the at least one application; and

generating a permission grant set for each code assembly that is a member of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application.

2. The method of claim 1 further comprising evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

3. The method of claim 1 wherein evaluating application evidence is based at least in part on an XrML license.

4. The method of claim 1 further comprising evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

5. The method of claim 1 further comprising evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

6. A method comprising generating a permission grant set for each code assembly that is a member of at least one application if application evidence for the at least one application satisfies at least one trust condition.

7. The method of claim 6 further comprising generating a permission grant set for each code assembly that is a member of a group of applications if application evidence for the group of applications satisfies at least one trust condition.

8. The method of claim 6 further comprising determining if the code assembly is a member of the at least one application.

9. The method of claim 6 further comprising receiving a manifest defining members of the at least one application.

10. The method of claim 6 wherein satisfying at least one trust condition is based at least in part on evidence provided with the at least one application.

11. The method of claim 6 wherein satisfying at least one trust condition is based at least in part on evidence external to the at least one application.

12. The method of claim 6 wherein satisfying at least one trust condition is based at least in part on an XrML license.

13. The method of claim 6 wherein satisfying at least one trust condition is based on evidence from user interaction.

14. The method of claim 6 wherein satisfying at least one trust condition is based on evidence from evaluation of previous trust decisions.

15. The method of claim 6 further comprising evaluating application evidence at an application level and a code assembly level before allowing the at least one application to execute.

1

2   16. The method of claim 6 further comprising evaluating application evidence at a

3   group level, an application level, and a code assembly level before allowing the at least

4   one application to execute.

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

17. A computer program product encoding a computer program for executing on a computer system a computer process, the computer process comprising:

receiving a manifest defining a plurality of code assemblies that are members of at least one application;

evaluating application evidence for the at least one application; and

generating a permission grant set for each code assembly that is a member of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application.

18. The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

19. The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence based at least in part on an XrML license.

20. The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

21. The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

22. A computer program product encoding a computer program for executing on a computer system a computer process, the computer process generating a permission grant set for each code assembly that is a member of at least one application if application evidence for the at least one application satisfies at least one trust condition.

23. The computer program product of claim 22 wherein the computer process further comprises generating a permission grant set for each code assembly that is a member of a group of applications if application evidence for the group of applications satisfies at least one trust condition.

24. The computer program product of claim 22 wherein the computer process further comprises determining if the code assembly is a member of the at least one application.

25. The computer program product of claim 22 wherein the computer process further comprises receiving a manifest defining members of the at least one application.

26. The computer program product of claim 22 wherein the computer process is based at least in part on evidence provided with the at least one application.

27. The computer program product of claim 22 wherein the computer process is based at least in part on evidence external to the at least one application.

28. The computer program product of claim 22 wherein the computer process is based at least in part on an XrML license.

29. The computer program product of claim 22 wherein the computer process is based on evidence from user interaction.

30. The computer program product of claim 22 wherein the computer process is based on evidence from evaluation of previous trust decisions.

31. The computer program product of claim 22 wherein the computer process further comprises evaluating evidence at an application level and a code assembly level before executing the at least one application.

32. The computer program product of claim 22 wherein the computer process further comprises evaluating evidence at a group level, an application level, and a code assembly level before executing the at least one application.

33. A system comprising:

a manifest defining at least one application;

application evidence for the at least one application;

a policy manager evaluating the application evidence relative to at least one

condition for trusting the at least one application, wherein the policy manager generates a

permission grant set for each code assembly that is a member of the at least one

application if the application evidence satisfies the at least one condition.

34. The system of claim 33 further comprising an XrML program authorization

module operatively associated with the policy manager for evaluating application

evidence including at least one XrML license.

35. The system of claim 33 wherein the policy manager evaluates evidence at a

group level, an application level, and a code assembly level before the at least one

application is executed.

36. The system of claim 33 further comprising a security policy specification

defining the condition.

37. The system of claim 33 wherein the policy manager further determines if the code assembly is a member of the at least one application.

38. The system of claim 33 wherein the application evidence is provided with the at least one application.

39. The system of claim 33 wherein the application evidence is provided external to the at least one application.

40. The system of claim 33 wherein the application evidence includes at least an XrML license.

41. The system of claim 33 wherein the application evidence includes evidence provided via user interaction.

42. The system of claim 33 wherein the application evidence includes evidence from the evaluation of previous trust decisions.

43. The system of claim 33 further comprising a security policy specification defining at least one trust condition for an application component, wherein the policy manager evaluates the at least one trust condition in the security policy specification.

44. A computer-readable medium having stored thereon a data structure, comprising:

a first data field specifying members of at least one application;

a second data field containing application evidence associated with the at least one application, wherein permission grant sets are generated for each member of the at least one application based on the application evidence.

45. The data structure of claim 44 wherein the first data field defines a group of applications.

46. The data structure of claim 44 further comprising a third data field identifying a location of one of the members of the at least one application.

47. The data structure of claim 44 further comprising a third data field specifying a requested level of trust for the at least one application.

48. The data structure of claim 44 further comprising a third data field requesting different levels of trust for different members of the at least one application.